Security method for transmissions in telecommunication networks

This application is a continuation of PCT/FI98/00721 filed 9-15-98.

Field of the invention

The invention relates to a method for providing connection security for transmission between the communicating parties in a telecommunication network.

Background of the invention

At the beginning of a communication a handshake is usually performed between applications in telecommunication networks, during which the parties involved typically authenticate each other and exchange key information, for example, negotiate an encryption algorithm and cryptographic keys to be used in communication. It is only after the handshake that the actual data is transmitted. The confidentiality of the transmission is arranged, for example, through ciphering. Figures 1a and 1b of the attached drawings show block diagrams of two known cipher algorithms which can be used to protect a transmission: a symmetric and a public key algorithm.

Figure 1a shows a symmetric algorithm based on a secret key shared between the participants. At party A's end the message M to be sent to party B is encrypted in box E of Figure 1a with the shared secret key K. The message is sent over a transmission route as encrypted cipher text C, which party B can decrypt in box D shown in Figure 1a with the same secret key K. Through decryption party B gets the original message M. An intruder eavesdropping transmission needs to know the secret key K in order to be able to read and understand the transmitted cipher text C. The encryption and decryption of the symmetric algorithm can be expressed by the equations:

$$C = E_K(M)$$
$$M = D_K(C),$$

where C is the cipher text, M is the message in plain text, E_K is the encryption with key K, and D_K is the decryption with key K.

Figure 1b shows a public key algorithm which is an asymmetric approach. This algorithm is based on two keys: a public key and a private key. These two keys are related in such a manner that a message encrypted with a public key K_+ can only be decrypted with the corresponding private key K_- and vice versa. In Figure 1b a message M is encrypted at party A's end in

box E with the public key K_+ of the intended receiver, that is party B. The encrypted cipher text C is transmitted over a transmission line to party B's end, where the cipher text C is decrypted in box D with the corresponding party B's private key K_- and the original message M is retrieved. The encryption and decryption of the asymmetric algorithm can also be expressed by the following equations:

$$C = E_B^+(M)$$

$$M = D_B^-(C),$$

where C is the cipher text, M is the message in plain text, E_B^+ is encryption with the receiver's public key K_B^+, and D_B^- is decryption with the receiver's private key K_B^-.

In the public key algorithm the encryption of a message with the private key K_- of the message sender acts as a signature, since anyone can decrypt the message with the known public key K_+ of the sender. Since asymmetric keys are usually much longer than symmetric keys, the asymmetric algorithm requires much more processing power. Thus asymmetric algorithms are unsuitable for encrypting large amounts of data.

A hybrid cryptography uses both the above-mentioned algorithms together. For example, only session keys are exchanged using public key algorithm, and the rest of the communication is encrypted with symmetric method.

To provide message integrity and authentication in a connection, a message authentication code MAC is calculated and attached to the transmitted message. For example, MAC can be calculated with a one-way hash algorithm in the following way:

$$h = H(K, M, K),$$

where K is the key, M is the message, and H is the hash function. The input cannot be deduced from the output. When MAC is attached to a message, the message cannot be corrupted or impersonated. The receiving party calculates MAC using the received message and the same hash function and key as the transmitting party and compares this calculated MAC to the MAC attached to the message in order to verify it.

Figure 2 shows examples for communication connections. A mobile station MS operating in the GSM network (Global System for Mobile communications) is able to make a connection to a bank directly from the GSM net-

work. Other possible connections presented in Figure 2 are connections from the GSM network to different services via gateway GW and Internet. In mobile communication networks, such as the GSM, the air interface from the mobile station MS to the GSM network is well protected against misuse, but the rest of the transmission route is as vulnerable as any other public telephone network, providing measures are not taken to provide connection security.

One problem with providing connection security is that handshaking requires plenty of processing time since several messages must be sent between the parties involved. The low processing power and narrow bandwidth in the mobile stations make handshakes particularly burdensome in mobile communication networks. Handshakes are also burdensome for applications which have numerous simultaneous transactions, for example, a server in a bank. Therefore, it is desirable to minimize the number and duration of the handshakes. This leads to the problem that an attacker has lots of time for cryptanalysis, as the same encryption keys are used between the two handshakes. If the attacker succeeds in the cryptanalysis, he can access all the material sent between the two handshakes.

Summary of the invention

The object of this invention is to provide a method for securely protecting transmitted information between communicating applications, especially over narrow-band connections, without unnecessarily loading the communicating parties.

This is achieved by using a method according to the invention characterized by what is stated in the independent claim 1. Special embodiments of the invention are presented in the dependent claims.

The invention is based on the idea that the communicating parties recalculate the security parameters during the transmission session simultaneously with each other at agreed intervals and the continue communicating and providing connection security for messages with these new parameters. The communicating parties monitor the time for recalculation and at the agreed intervals recalculate and thus change the security parameters without a handshake taking place. In the primary embodiment of the invention, the messages are numbered and the number agreed on triggers recalculation at intervals.

4

The advantage of the method according to the invention is that security parameters can be changed during the session without handshaking. This reduces the need for handshakes.

Another advantage of the method according to the invention is that the security of the transmission is improved, i.e. attacking is made more difficult and less profitable.

Brief description of the drawings

The description of the preferred embodiments of the invention will now be made with reference to the attached drawings, in which

Figure 1a shows a symmetric ciphering algorithm as a block diagram;

Figure 1b shows an asymmetric ciphering algorithm as a block diagram;

Figure 2 gives a few examples of connections from a mobile communication network to some applications;

Figure 3 shows session keys providing connection security for transmitted messages according to the primary embodiment of the invention; and

Figure 4 shows the primary embodiment of the invention as a flowchart.

Detailed description of the invention

The present invention can be applied to any telecommunication network. Below the invention is described in more detail using as an example a mobile station operating in the digital GSM mobile communication system and communicating with an application located either inside or outside the GSM network.

In the following the primary embodiment of the invention is described in more detail with reference to Figures 2, 3 and 4.

Figure 2 shows example connections as described earlier. The mobile station MS contacting the server in the bank first performs a handshake according to the prior art, during which both the MS and the bank may authenticate the other and exchange any session key information needed. According to the invention, for example, during the handshake, a mobile station and an application in the bank negotiate and agree on appropriate intervals for recalculating the security parameters to be used to provide privacy, data integrity and authentication during the communication. For example, the negotiation can be implemented so that each of the communicating parties,

i.e. in the example in Figure 2 the mobile station MS and the application in the bank, propose a suitable interval for recalculation and one of the proposed intervals is chosen and agreed upon, for example, the one that is more frequent. Examples for suitable parameters to determine intervals are a message sequence number, such as every fourth message, or a suitable time period. Even if handshaking is not needed and therefore not performed at the beginning of the communication session, according to the invention the communicating parties still need to agree on recalculation intervals.

After agreeing on the intervals for recalculation both the parties monitor the agreed intervals. If an interval after four messages is agreed on, either both parties monitor the number of messages sent, which requires a reliable transmission media with no lost messages, or they number all transmitted messages and transmit these sequence numbers with the messages. The advantage of sending the sequence numbers or time stamps with the messages is that the recalculation is synchronous at both ends even though some messages get lost along the way or messages received are not in correct order. When in the example described above the fourth message is transmitted and received, both the communicating parties recalculate the security parameters and use these new parameters for providing connection security for the next four messages. A handshake or any other session key exchange is not performed during or after the recalculation of the parameters. The recalculation can be based on a shared secret and the latest sequence number, for example. Security parameters can also be used to calculate session keys Kn for ciphering and the message authentication code MAC in the following way, for example:

$$Kn = H(S, N)$$

$$MAC = H(M, S, N),$$

where H is a predetermined hash algorithm, S is the shared secret, N is the latest sequence number, and M is the message to be transmitted in plain text.

Figure 3 shows an example of changing the session key according to the invention. In Figure 3 the messages sent from the MS are numbered with the sequence numbers 0 to 3. In the example in Figure 3, the interval for recalculation is agreed to be after two sent messages. The message with sequence number 0 is sent to the bank encrypted with session key K1. The application in the bank decrypts the message 0 with the same session key

6

K1 when symmetric algorithm is applied in ciphering. The message with sequence number 1 is also sent encrypted with session key K1. As the mobile station MS has now sent two messages, both the MS and the application in the bank recalculate the security parameters, for example, the session key K2, using the shared secret and the latest sequence number that is 1. After recalculation the MS sends the next message 2 to the bank encrypted with session key K2. The application in the bank decrypts the message 2 with the same recalculated session key K2. Also the message 3 is encrypted with session key K2 before transmission. After that the MS and the application in the bank again notice that the agreed interval has been reached and both parties recalculate the security parameters, for example, the session key K3, using the shared secret and the latest sequence number 3.

Figure 4 shows the primary embodiment of the invention as a flowchart. At the beginning of a communication at step 41, the parties involved in communication, in the example in Figure 2 the MS and the application in the bank, negotiate and agree on the interval for security parameters recalculation. As in the example described above, we again assume that the interval is agreed to be after two transmitted messages. Both communicating parties keep track of the number of transmitted messages, for example, with counters at each end. At stage 42 one of the communicating parties, for example, the MS, encrypts the first message to be sent with a session key K1 obtained from the shared secret that was exchanged during the handshake or otherwise shared with the parties involved. The encrypted message is sent and the receiving party decrypts the message with corresponding session key K1 (stage 43). At this time the counter is set at 1. At stage 44 both parties, in this example the MS and the application in the bank, check whether the agreed interval has been reached by checking whether the value in the counter is equal to the value of the agreed interval, for example. As the message sent was only the first message, recalculation does not take place yet, and the next message is encrypted and decrypted with the same session key K1. When two messages have been sent, and the counters indicate the value 2 which corresponds to the value of the agreed interval, the clause at stage 44 becomes true and both communicating parties recalculate security parameters in a predetermined manner and obtain a new session key K2 (stage 45). At stage 46 the interval monitoring is reset, i.e. the message count is restarted, for example, by setting the counter to 0. At stage 47 a

7

check is made as to whether there are still more messages to be sent, and if so the encryption of a message is continued at stage 42 with the first message to be encrypted using the latest session key K2, after which the message is sent and the counters may be set to value 1. The process continues in similar manner until all the messages to be sent are transmitted.

In another embodiment of the invention, MAC is used to provide connection security for message transmission in the place of ciphering. According to the invention MAC is calculated, from the sequence number that last triggered recalculation of the security parameters, for example. In the example in Figure 3, MAC is calculated with the sequence number 1 for the messages shown as encrypted with K2 and with the sequence number 3 for the messages to be encrypted with K3. Otherwise this other embodiment of the invention is implemented in the same fashion as in the first embodiment described above.

Yet another embodiment of the invention uses ciphering and MAC to provide connection security for messages. This is implemented by combining the embodiments described above.

Recalculation of the security parameters includes also the possibility of changing the ciphering algorithm to be used in ciphering the next messages.

The drawings and the accompanying explanation are only intended to demonstrate the principles of the invention. The details of the method according to the invention can vary within the patent claims. Although the invention was described above mostly in connection with a mobile station and service application communication, the invention can also be used for providing connection security for messages between any two or more applications communicating together, also in mobile to mobile connection in a speech, data and short message transmission. The invention is also suitable for use in recalculating other security parameters than session keys and MACs. The invention is not restricted for use only in connection with the ciphering algorithms presented above, but can be applied together with any ciphering algorithms.

8